3 システムのセットアップ

本体のセットアップを終了したら、システムのセットアップをします。システムのセットアップは購入後、初めてセットアップする場合と再セットアップする場合に分けて説明しています。

RealSecureについて

RealSecureシステムはリアルタイムの侵入検出およびレスポンスの自動システムでコンピュータシステムやネットワークのアクティビティを目立たないように分析します。

RealSecureのコンポーネント

RealSecureには下記のコンポーネントがあります。

- **Network Sensor**
  - Sensorはネットワークのトラフィックを監視して、攻撃やその他のセキュリティ関連イベントを検出します。
  - イベントが発生すると、Sensorがイベントに反応し、ユーザに通知します。
- **管理コンポーネント**

  管理コンポーネントには2つの管理ソフトウェアがあります。

  - Workgroup Manager
  - SiteProtector

  これらのコンポーネントにより、コンソールから視覚的にイベントを監視したり、1つ以上のEventCollectorを使用して、Sensorからデータを収集したりします。

EventCollectorとは？

EventCollectorは次の目的を持っています。

- Sensorからのイベントをデータベースに保存する。
- SensorからのイベントをConsole上に出力する。

ただし、設定によってデータベースへの書込みやConsole上への出力をしないようにすることもできます。

管理コンポーネントの選択基準を以下に示します。

- Workgroup Manager

  管理用に使用する装置のCPUスペックやSQLServerが準備できないなど、システム要件に合わせてWorkgroup Managerをご使用ください。なお、Workgroup Manager Ver.6.7では、256Mバイトのメモリ容量が最低限必要です。

- SiteProtector

  他の脆弱性検出製品などと連携した監視など、より高度な管理機能を必要とする場合は、SiteProtectorを選択します。

システム要件は下記URLを参照してください。

【Workgroup Manager】

http://www.isskk.co.jp/product/RS/RS7sysreq.html

【SiteProtector 2.0】

http://www.isskk.co.jp/product/RS/RSSP20_sysreq.html

最新製品のダウンロード

本装置を使用する為には、管理コンポーネントに本装置を登録する必要があります。そのため、管理コンポーネントをインストールするコンピュータが別途必要です(システム要件につきましては、この章の「RealSecureコンポーネント」を参照してさい)。

本体添付のRealSecureプロダクトCDには、出荷時点での最新版の管理コンポーネントが格納されていますが、最新の攻撃や機能のアップデートに対応するため、常に最新版を使用することをお勧めします。
最新版を入手するためには、以下の手順を行ってください。

① ダウンロードサイトへのアクセス

次のURLへアクセスしてください。

https://www.isskk.co.jp/download/Down.html

(このサイトは、RealSecure 開発元であるインターネットセキュリティシステムズ(ISS)社のサイトです)

② ソフトウェア使用許諾契約書の同意

製品の最新版をダウンロードするには、ソフトウェア使用許諾契約書に同意する必要があります。

また、製品をダウンロードする際にはIDとパスワードが必要です。IDとパスワードについては本体に添付の「セットアップカード」に記載されています。

③ 製品のダウンロード

管理コンソールとして下記製品をダウンロードしてください。

- SiteProtector(原則としてSQLServerを別途用意してください)
- Workgroup Manager(必要に応じて「MSDE2000 English」もダウンロードください)

SiteProtectorとWorkgroup Managerはいずれか一方を選択してください。選択基準については、前述の説明を参照してください。

システムのセットアップ

最新マニュアルのダウンロード

本製品のリファレンスマニュアルは、RealSecureパッケージCD-ROMに格納しています。
詳細な使用方法については、リファレンスマニュアルを参照してください。
最新のマニュアルは、URLから入手することができます。
ダウンロードしたい製品マニュアルを検索してください。

URL:　http://www.isskk.co.jp/eval/manuals.html

なお、マニュアルはAdobe Acrobat Readerで閲覧できるPDF形式です。
Arcrobat Readerがインストールされていないときは、「保守・管理ツール」の[ソフトウェアのセットアップ]の[Acrobat Reader]を選択して，Acrobat Readerをインストールしてください。

マニュアルの内容紹介

本製品に関するマニュアルを以下に示します(これらのマニュアルは2003年4月4日現在のものです)。各製品マニュアルの目次を付録に掲載しています。参照してください。

今後のマニュアルの新規追加・更新は下記URLを参照の上、ダウンロードしてください。

URL:　http://www.isskk.co.jp/eval/manuals.html

- RealSecure Network Sensor 7.0
  - RS_NetSensor_IG_7.0j2.pdf (インストールガイド　日本語版)
  - RS_NetSensor_PG_7.0j.pdf (ポリシーガイド　日本語版)
- RealSecure WorkgroupManager 6.5&6.7
  - RS_WGM_IG_6.5j.pdf (インストールガイド日本語版)
  - RS_WGM_UG_6.5j.pdf (ユーザガイド日本語版)
  - RS_WGM_UG_6.7.pdf (ユーザガイド・目次のみ日本語版)
  - RS_WGM_IG_6.7.pdf (インストールガイド・目次のみ日本語版)
- RealSecure SiteProtector 2.0
  - rsspigInstallationandImplementationj.pdf (インストールガイド日本語版)
  - Migration_of_WGM_to_RSSP.pdf (マイグレーションガイド・目次のみ日本語版)
  - rssprgReferenceGuide.pdf (リファレンスガイド・目次のみ日本語版)
  - rsspStrategyGuide.pdf (ストラテジーガイド・目次のみ日本語版)
  - rssptsTroubleshooting.pdf (トラブルシューティングガイド・目次のみ日本語版)
  - rsspUpgradeDoc.pdf (アップグレードガイド・目次のみ日本語版)

初めてのセットアップ

購入後、初めて本製品をセットアップする時の手順について説明します。

セットアップの概要

本製品のセットアップには、本体以外にマシンや接続のためのケーブルなどが必要です。また、それぞれのマシンについてもソフトウェアのインストールなど準備が必要です。

- **本体**

  RealSecure Network Sensor(Linux版)のモジュールがインストール済みです。後述のシステムのセットアップの手順に従ってセットアップを行ってください。

- **コンソール用PC**

  本体のコンソール用PCです。シリアルケーブル(クロス)を使用して本体と接続し、本体のセットアップを行います。

- **管理PC**

  本体(RealSecure Network Sensor)の管理・監視するためのマシンです。

以下に、セットアップの流れを示します。

1. システムのセットアップ
   - 1.1 ハイパーターミナルなどの通信ソフトウェアの確認
   - 1.2 シリアルケーブル(クロス)の接続
   - 1.3 ターミナルエミュレータの設定
   - 1.4 コンソール用PCの接続
   - 1.5 本体のIPアドレス、ホスト名の設定
   - 1.6 設定コマンド(setup.sh)によるNetwork Sensorの設定
   - 1.7 RealSecureサービスの起動
2. 管理ソフトウェアのインストール
   - 2.1 データベースのインストール
   - 2.2 管理ソフトウェアのインストール
   - 2.3 パッチの適用

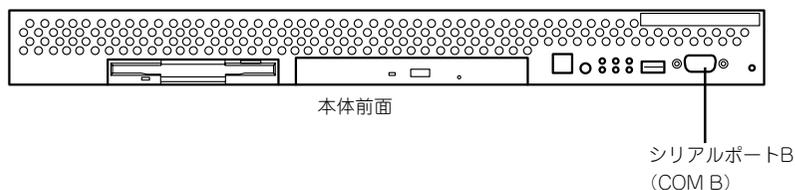
コンソール用PCのセットアップと接続

本体の電源がOFFの状態で、コンソール用PCを本体前面にあるシリアルポートB(COM B)に接続し、システムを起動してください。

1. 本体に接続するために必要なもの

- シリアルインタフェース(RS-232C)を持ったコンピュータ
- 通信用ソフトウェア(例: Windows 98ハイパーターミナル)
- シリアルケーブル(クロス)(K410 - 84(05))

2. ケーブルの接続

本体前面にあるシリアルポートB(COM B)にシリアルケーブル(クロス)を接続してください。

3. ターミナルエミュレータの設定

シリアルコンソールの速度(ボーレート)は、19200に設定してください。

4. コンソール用PCの接続

本体の電源をONにした後、しばらく(3分程度)してからコンソール用PCの<Enter>キーを押すと、コンソール用PCのディスプレイにloginプロンプトが表示されます。

コンソール用PCから「root」と入力し、「Password」に同梱の「管理者用パスワード」に書かれているパスワードを入力します。

> 重要 **rootのパスワードは、「passwd」コマンドで出荷時のパスワードから変更してください。**

以上でコンソール用PCの接続ができました。以降の説明では、コンソール用PCからの操作でシステムをセットアップしていきます。

システムのセットアップ

本装置のホスト名、IPアドレス、およびRealSecure Network Sensorに対してKey Administratorの設定をします。

rootでログインした後、以下の手順に従ってセットアップを行ってください。

IPアドレスとホスト名の設定

管理ソフトウェアとの通信用にIPアドレスを設定します。まず、本体背面のLANポート1とLANポート2にネットワークケーブルを接続してください。ここで、管理ソフトウェアとの通信インターフェースデバイスは、必ずeth0としてください。

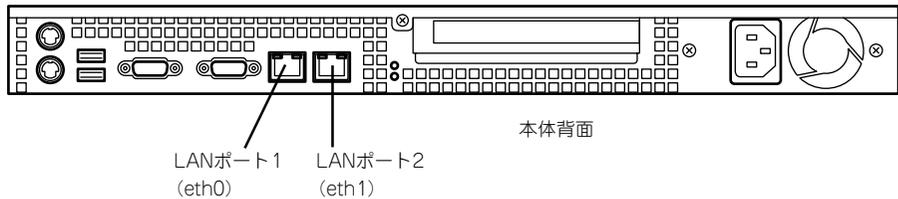
1. /etc/hosts ファイルを変更し、ホスト名とIPアドレスを設定する。

   以下に/etc/hostsファイルの例を示します。なお、デフォルトで書かれている127.0.0.1に対する設定は削除してください。

   192.168.0.10　sensor.domain.com sensor

   重要

   管理ソフトウェアとの通信は、LANポート1(eth0デバイス)を使用してください。対象とするネットワークセグメントの監視ポートには、LANポート2(eth1デバイス)を使用してください。

   なお、LANポート2はステルス設定となっているため、管理ソフトウェアと通信することはできません。

2. 「netconfig」コマンドでIPアドレスを設定する。

   管理ソフトウェアとの通信用にeth0に対して設定します。以下のように引数を指定し「netconfig」コマンドを実行します。後は画面の指示に従ってIPアドレスを設定してください。

   % netconfig --device eth0

3. 本装置を再起動する。

   以下のコマンドを実行して本体を再起動し、これまでに設定したネットワーク設定を有効にします。

   % reboot

   再起動後、「ifconfig」コマンドを使用して設定したIPアドレスが正しく表示されるかを確認してください。

   % ifconfig eth0

RealSecure Network Sensorの設定

コンポーネントのセットアップをします。

1. 以下のコマンドを続けて実行し、セットアップシェルを起動する。

   % cd /opt/ISS/issSensors/network_sensor_1/
   % ./setup.sh

   その後、画面の指示に従い以下のように設定してください。なお、詳細については「RealSecure パッケージCD-ROM」に入っている「RealSecure Network Sensor and Gigabit Network Sensor Installation Guide7.0 日本語版」の6章を参照してください。以下、その設定例を示します。

   ① [Setup Key Administrator]オプションを選択する。

   管理コンピュータのマシン名とユーザ名を入力します。

   例） mgrcomputer_administrator

   ② [Allow Auto-Import of console and Event Collector keys]オプションを選択する。

   自動キーインポート機能の有効・無効が選択できます。通常、「on」にしてください。「on」にすると、管理ソフトウェアとの通信手順を簡略化させることができます。

   ③ [Generate Encryption Keys]オプションを選択する。

   暗号キーを生成します。

   ④ <Q>キーを押してセットアップを終了する。

   なお、本製品はOSインストール時にファイアウォールの設定をしていない([None]を選択)ため、「4) Edit RedHatp ipchains rules」での設定は必要ありません。

2. 以下の順にコマンドを実行してRealSecureサービスを再起動する。

   % service realsecure stop
   % service realsecure start

サービスの起動後、「ISS Daemon starting.」というメッセージが表示されることを確認してください。

以上でセットアップは完了です。
以降の説明では、管理PCに管理ソフトウェアをインストールします。

システムのセットアップ

管理ソフトウェアのインストールおよび設定手順

管理用マシンに管理ソフトウェアをインストールします。
ここでは、追加コンポーネントを手配せずに使用できるWorkgroup Managerの標準インストールを例にとり説明します。
Workgroup Managerは現在(6月2日時点)Ver.6.7が最新版となります。以下の手順では、いったんVer.6.5をインストールした後、Ver.6.7にアップグレードする方法を説明します。最新版へのアップデートを行うためには、メンテナンス製品を購入し、キーコードの発行をあらかじめ受けておく必要があります。

ここではインストールの主な流れを紹介します。
詳細なセットアップ方法については、「RealSecureパッケージCD-ROM」に入っている下記のマニュアルを参照してください。

- SiteProtectorの場合: rsspigInstallationandImplementationj.pdf
- Workgroup Manager: RS_WGM_IG_6.5j.pdf

1. MSDE2000のインストール

MSDE2000は「RealSecureパッケージCD-ROM」に格納されています。

「<CD-ROMドライブ>:¥packages¥WGM¥msde2000.exe」を実行してください。

2. WorkgroupManager 6.5のインストール

WorkgroupManager 6.5は「RealSecureパッケージCD-ROM」に格納されています。

「<CD-ROMドライブ>:¥packages¥WGM¥RealSecureWorkgroupManager65.exe」を実行してください。

3. Enterprise Databaseに対するパッチの適用

本パッチは「RealSecureパッケージCD-ROM」に格納されています。

RealSecure パッケージCD-ROMの「RS061202.html」をお読みになった上で、「<CD-ROMドライブ>:¥packages¥patch¥Enterprise¥RealSecure6.xDatabasePatch.exe」を実行してください。

4. MSDE2000のSP3パッチの適用

本パッチは「RealSecureパッケージCD-ROM」に格納されています。本パッチは以下の手順に従って適用してください。

① 「<CD-ROMドライブ>:¥packages¥patch¥SQL_SP3¥SQL2KDeskSP3.exe」を実行する。

② 展開先フォルダの確認で、適切なフォルダを指定する。

③ EventCollectorが停止していること、およびWorkgroupManagerが起動していないことを確認する。

④ コマンドプロンプトを起動し、以下のフォルダに移動する。

<展開先フォルダ>¥MSDE¥

⑤ コマンドプロンプトより、以下のように入力してsetup.exeを実行する。

setup.exe /upgradesp sqlrun

⑥ インストール後、マシンを再起動する。

5. WorkgroupManager 6.5から6.7へのアップデート

アップデートモジュールは、「RealSecureパッケージCD-ROM」に格納されています。

RealSecure パッケージCD-ROM の「WGM67_Update_Flow.doc」をよくお読みになった上で、「<CD-ROMドライブ>:¥packages¥WGM¥RSWGM67Upgrade¥setup.bat」を実行してください。Flow.docを開くためのアプリケーションやDLLなどはお客様で用意してください。

6. EventCollectorのサービスリリース(SR)の適用

インターネットに接続できることを確認してください。

管理ソフトウェアのコンポーネントであるEventCollectorを最新の状態にアップデートします。

Workgroup ManagerからEventCollectorを選択し、右クリックして「X-Press or Product update」を選択してください。

インターネットアドレスに下記のURLを入力し接続してください。

URL: http://www.isskk.co.jp/update/RealSecure

7. Network SensorへのX-Press Update(XPU)の適用

本装置にインストールされているRealSecure Network Sensorを、最新の状態にアップデートします。

Workgroup ManagerからNetwork Sensorを選択し、右クリックして「X-Press or Product update」を選択してください。

インターネットアドレスに下記のURLを入力し接続してください。

URL: http://www.isskk.co.jp/update/RealSecure

8. Workgroup Managerヘルプ、レポート、イベント日本語化

初期状態ではヘルプ、レポート、イベントは英語で出力されます。

英語で出力するメッセージを日本語で参照したい方は、下記URLより、a)～c)の日本語版(ヘルプ、レポート、イベント)をダウンロードしてください。

URL: https://www.isskk.co.jp/download/Jpn.html#RealSecure6.6

a) 導入方法: RS 6.6 日本語ヘルプ導入方法(必ずお読み下さい)
製品名: RS 6.6 日本語ヘルプ

b) 導入方法: RS 6.6/6.5 日本時間レポート導入方法(必ずお読み下さい)
製品名: RS 6.6/6.5 日本時間レポート

c) リリースノート: RS7.0 NWS XPU 20.1-20.7 リリースノート
製品名: RS7.0 NWS XPU 20.1-20.7 日本語版

9. LANポート2(eth1)のステルス設定

EventCollectorとNetworkSensorのAssetsを作成された後に、以下の手順に従ってNetworkSensorの監視ポートをeth1に設定してください。

詳細については、「RealSecureパッケージCD-ROM」に含まれているNetworkSensor 7.0のインストールガイドを参照してください。

① 「Managed Assets」ウィンドウで、[Asset]→[Manage]で[NetworkSensor]を選択する。

② 「Managed Assets」ウィンドウに表示されたNetworkSensorを右クリックして[Set console as master controller]を選択する。

③ 再度、NetworkSensorを右クリックして [Properties]を選択する。

NetworkSensorのプロパティウィンドウが表示されます。

④ [Adapters]タブをクリックし、「Adapter of Monitored Network」の項目でService Nameが「eth1-p」の行を選択する。

⑤ 「Adapter to Send Kills」の項目でService Nameが「eth1-p」の行を選択する。

⑥ [OK]をクリックしてウィンドウを閉じる。

「Managed Assets」ウィンドウに表示されたNetworkSensorの「Component Status」に「Updating」と表示され、それが元の表示に戻れば設定完了です。

⑦ 「Adapter to Send Kills」の項目でService Nameに「eth1-p」を選択する。

⑧ 再びNetworkSensorのプロパティウィンドウで、④と⑤の設定が保存されていることを確認する。

X-Press Update最新情報メールの申込み

本製品では、最新の攻撃に対応するためのアップデートが作成されています。このアップデートのことを「X-Press Update」と呼んでいます。
X-Press Update日本語版の提供開始をメールにてお知らせするメール配信サービスを提供しています。

X-Press Updateの提供の際、メールによるご案内をご希望される方は下記URLよりお申し込みください

URL: https://www.isskk.co.jp/support/XPressUpdates/xpuentry.html

ESMPRO/ServerAgentのセットアップ

ESMPRO/ServerAgentは出荷時にインストール済みですが、固有の設定がされていません。以下のオンラインドキュメントを参照し、セットアップをしてください。

添付のバックアップCD-ROM:/nec/Linux/esmpro/doc/users.pdf

ESMPRO/ServerAgentの他にも「エクスプレス通報サービス」(4章参照)がインストール済みです。ご利用には別途契約が必要となります。詳しくはお買い求めの販売店または保守サービス会社にお問い合わせください。

シリアル接続の管理PCから設定作業をする場合は、管理者としてログインした後、設定作業を開始する前に環境変数「LANG」を「C」に変更してください。デフォルトのシェル環境の場合は以下のコマンドを実行することで変更できます。

```
# export LANG=C
```

システム情報のバックアップ

システムのセットアップが終了した後、添付の「保守・管理ツールCD-ROM」にあるオフライン保守ユーティリティを使って、システム情報をバックアップすることをお勧めします。システム情報のバックアップがないと、修理後にお客様の装置固有の情報や設定を復旧（リストア）できなくなります。次の手順に従ってバックアップをしてください。

重要 **保守・管理ツールCD-ROMからシステムを起動して操作します。保守・管理ツールCD-ROMから起動させるためには、事前にセットアップが必要です。4章を参照して準備してください。**

1. 3.5インチフロッピーディスクを用意する。
2. 本体に添付の「保守・管理ツールCD-ROM」から「オフライン保守ユーティリティ」を起動する。

   「保守・管理ツールCD-ROM」の使い方については4章を参照してください。
3. ［システム情報の管理］から［退避］を選択する。

   以降は画面に表示されるメッセージに従って処理を進めてください。

続いて管理PCに本装置を監視・管理するアプリケーションをインストールします。次ページを参照してください。

管理PCのセットアップ

本装置をネットワーク上のコンピュータから管理・監視するためのアプリケーションとして、「ESMPRO/ServerManager」と「Management Workstation Application（MWA）」が用意されています。
これらのアプリケーションを管理PCにインストールすることによりシステムの管理が容易になるだけでなく、システム全体の信頼性を向上することができます。

ESMPRO/ServerManagerとMWAのインストールについては4章、または保守・管理ツールCD-ROM内のオンラインドキュメントを参照してください。

再セットアップ

再セットアップとは、システムクラッシュなどの原因でシステムが起動できなくなった場合などに、添付の「バックアップCD-ROM」を使ってハードディスクを出荷時の状態に戻してシステムを起動できるようにするものです。以下の手順で再セットアップをしてください。

重要 **再インストールを行うと、装置内の全データが消去され、出荷時の状態に戻ります。必要なデータが装置内に残っている場合、データをバックアップしてから再インストールを実行してください。**

再インストールには、本体添付のバックアップCD-ROMとバックアップCD-ROM用インストールFDが必要です。
「バックアップCD-ROM用インストールFD」を3.5インチフロッピーディスクドライブに、「バックアップCD-ROM」をCD-ROMドライブにそれぞれセットして、POWERスイッチを押して電源をONにします。
しばらくすると「バックアップCD-ROM用インストールFD」から設定情報を読み取り、自動的にインストールを実行します。

重要 **このとき、確認などは一切行われずにインストール作業が開始されるため、十分注意してください。**

約30分程度でインストールが完了します。インストールが完了したら、CD-ROMが自動的にイジェクトされます。CD-ROMとフロッピーディスクの両方をドライブから取り出してください。最後に、POWERスイッチを押して電源をOFFにしたら終了です。

40分以上待っても、CD-ROMがイジェクトされず、CD-ROMへのアクセスも行われていない場合は再インストールに失敗している可能性があります。リセットして、CD-ROMとフロッピーディスクをセットし直して、再度インストールを試みてください。
それでもインストールできない場合は、保守サービス会社、またはお買い上げの販売店までご連絡ください。

インストール後、前述の「システムのセットアップ」を参照して作業を進めてください。